Department of Commerce Technical Reference Model and Standards Profile Framework

Technical Reference Model Introduction

The objective of a Technical Reference Model (TRM) is to define the building blocks for developing an Information Technology (IT) Architecture. A TRM provides a common conceptual framework, defines a common vocabulary, and provides a set of service definitions and relationships. It is a generally-accepted representation of the generic components of an IT system and is derived from the *NIST Special Publication 500 – 230, Application Portability Profile, Version 3.0*.

The use of a TRM allows an Operating Unit to better control and coordinate development, acquisition, interoperability, and support of its IT systems. It does this by guiding the design and development of IT systems to meet the Unit's specific mission and business needs. The TRM allows designers, developers, and users to agree on definitions, have a common understanding of the services to be provided, and identify and resolve issues affecting interoperability, portability, and scalability.

The TRM describes the main elements of a complete IT system as a set of IT Services. The Department of Commerce has identified eleven IT service categories. Each service category is further divided into service components that may support that category. The TRM defines not only technologies currently in use, but also those that could potentially be used in the future. The IT Services may be implemented on a single computer or on a collection of homogeneous or heterogeneous computing platforms. The TRM can be tailored to support a wide range of requirements, and an organization can add Service Categories or Components it deems necessary.

The associated Standards Profile provides a framework for specifying standards for these service components. A limited number of mandatory standards are identified, while other standards are recommended. Except for mandatory standards, an Operating Unit can use the Standards Profile to specify standards it needs for its specific business and technical needs.

IT Services

An IT Service Category is a higher level abstraction that consists of a collection of service components organized to accomplish a specific function or set of functions. A service component is made up of standards, interfaces, protocols and product specifications.

The following IT Services are recommended to be included in the TRM and are defined below:

- Networking
- Security
- Operating System
- User (Person)/Computer Interface
- Data Management
- Data Interchange
- Multimedia/Graphics
- Communications
- Document Management
- Support
- Hardware.

An Operating Unit can choose to define its IT Services differently.

Networking Services

Network services provide connectivity and basic services to foster communications across workgroups and sites. These services comprise the network infrastructure to provide the capabilities and service components to support distributed data access and interoperability in a heterogeneous environment. Service components for this category may include Network Management, Address Management, Internet Protocol (IP) Suite and Routing Protocols. Network applications, such as HTTP, FTP, E-mail, are grouped under Communication Services.

Security Services

The IT architecture should follow an accepted set of security services in order to ensure the integrity of mission critical information. Information security services are necessary to protect the IT infrastructure from a hostile environment and to protect sensitive information contained within an information system. The appropriate level of protection is determined based upon the value of information to the business owner and the perceived possible threats to the information. The service components for implementing information security services may include the following:

- Identification, Authentication, and Non-repudiation
- Audit Trail Creation and Analysis
- Access Controls
- Cryptography Management
- Virus Protection
- Fraud Prevention
- Detection and Mitigation
- Intrusion Prevention and Detection

Operating System Services

Operating system services provide the software environment and base interfaces within all computing devices to function while maximizing machine resources and capabilities. Operating system service components may include Kernel Operations, Fault Management, Shell and Utilities, and Backup and Recovery.

User (Person)/Computer Interface Services

User (person)/computer interfaces are the most visible to the user. Significant advances have been made in interface technology in ease of use and reducing the development effort required. Depending on the capabilities required by users and the applications, these service components may include Dialogue Support, Window Management, and Multimedia Specifications. This area also defines accessibility compliance and the methods by which people can interact with an application.

Data Management Services

Data management services encompass the procedures, practices, methods, and software used to manage data.. These services support definition, storage, and retrieval of data elements. Data management services also include query and security of data, and structures of information systems. Data management service components provide the functions to establish Meta Data, Data Dictionary, Directory Services, Database Management Systems, and access to distributed data.

Data Interchange Services

Data interchange services provide specialized support for the exchange of information, and may include such service components as Document Markup Language, Format, Tag Set, Data Element Standardization, Geographic Information Systems (GIS), and File Transfer between applications on the same or diverse platforms. The rapid growth of the Internet has led to the development of data interchange formats for text and graphics and multimedia.

Multimedia/Graphics Services

Multimedia/graphics services provide the capability to manipulate and manage information consisting of text, graphics, images, video, and audio. These services can be used directly or they can also be used by other support applications to satisfy a common requirement. These services can be used in combination or separately. This service also provides interfaces for programming

two-and three-dimensional graphics in a device-independent manner. Multimedia/Graphics service components may include:

- Raster Graphics
- Vector Graphics
- Audio Compression/Streaming
- Video Compression/Streaming
- Multimedia-processing (including all or any combination of the above-mentioned media, and to perform these actions on two or more types of media simultaneously.)

Communications Services

Communications services provide the capability to send, receive, forward, and manage electronic and voice messages. They also provide real-time information exchange services in support of conferences. The service components may include:

- Directory Access
- E-Mail
- Messaging
- Work Flow Management
- Calendaring
- Enhanced Telephony
- Shared-screen Teleconferencing
- Videoconferencing
- Broadcast

Document Management Services

Document management services formulate the process of managing documents through their life-cycle. Document management services may be associated with the following service components: Creating, Retrieving, Publishing and Archiving.

Support Services

Support services include those IT components where human intervention from a third party is required. Examples of support service components may include: IT Training, Help Desk, and Hardware Installation and Maintenance.

Hardware Services

Hardware Services are generally very specific to the application, user and capacity requirements for a system. Hardware Services may pertain to such service components as the Processing Platforms (Client, Application and Data), Peripherals, Mobile Platforms and Storage. Hardware-

based services also include the interfacing, embedded software services provided by device drivers. Hardware interfaces with operating system and network services must be compatible.

Standards Profile Format

Table 1 exhibits the suggested Department format for the Standards Profile of each Operating Unit. The Services column identifies the service and provides representative standards, interfaces, protocols and/or product specifications that fall within the Service Category. The Standards/Protocols column lists the particular vendor-neutral and vendor-specific Standards and/or Protocols cited for use by the Operating Unit for the particular Service Category. Standards, Protocols, or Specifications should be associated with individual service components (items listed under a service category), and not with a service category in general. If no Standard or Protocol is applicable or available, then Column 2 should be left blank for that particular service component or the service component deleted from the table. The Implementation Level Column will be used to indicate the level of compliance or adoption for the invoked standard. The following classifications will be used to describe the Implementation Level of Standards to an Operating Unit's Standards Profile:

- Mandatory
- Recommended
- Emerging
- Obsolete.

The four classification categories are defined below.

- **Mandatory**: Mandatory standards must be followed, adopted and used. Mandatory standards are required to comply with applicable laws, regulations, Departmental requirements, or because of industry technological practices or business processes. For instance, the TCP/IP protocol stack is considered a mandatory standard throughout the Federal Government, industry and academia. Each management level of the Department may impose mandatory standards on all units within its jurisdiction. In other words, the Department may impose mandatory standards on the Operating Units, the Operating Units may impose mandatory standards on regional offices and regional offices can impose mandatory standards on local organizations under its jurisdiction. Mandatory standards must be followed throughout the organization that defines and imposes the standard as well as all subordinate organizations. Additional mandatory standards can be added by lower-tiered organizations. However, mandatory standards cannot be disregarded when invoked by a higher level of organizational authority.

- **Recommended**: Recommended standards are those standards that are highly desirable and/or describe the minimum needed to implement a family of standards. They can be either extensions to mandatory or required standards, or be ad hoc standards used in areas

where no other mandatory standard has been identified. A recommended standard can be invoked as a mandatory standard at a lower level of the organization.

- **Emerging**: An emerging standard may involve a technology that is still evolving. An emerging standard may be in draft form or going through the peer review process. Also, an emerging standard may have been issued but the technological implementation of the standard may not be in a mature state. Emerging standards may be invoked at a lower level of an organization to allow technical flexibility at the level that it is invoked. Support and training for emerging standard is provided by the sponsoring organization.

- **Obsolete**: Obsolete standards are those standards or technologies that are currently part of the baseline, and that are recommended to be phased out and are not be procured. These standards may have been cancelled or superseded and may no longer be supported technically by any vendor. Obsolete standards may face interface-compatibility problems in the future.

Table 1 - Suggested Department Format for the Standards Profile of Each Operating Unit

Services	Standards/Protocols	Implementation Level
Networking Services		
Network Management Address Management IP Suite Routing Protocols		
Security Services		
Identification, Authentication, and Non-repudiation Audit Trail Creation and Analysis Access Controls Cryptography Management Virus Protection Fraud Prevention Detection and Mitigation Intrusion Prevention and Detection		

Services	Standards/Protocols	Implementation Level
Operating System Services		
Kernel Operations Fault Management Shell and Utilities Backup and Recovery		
User (Person)/Computer Interface Services		
Web-based Interfaces Accessibility		
Data Management Services		
Meta Data Data Dictionary Directory Services Data Base Management		
Data Interchange Services		
Document Markup Language Format Tag Set Data Element Standardization File Transfer Geographic Information Systems		
Multimedia/Graphics Services		
Raster Graphics Vector Graphics Audio Compression/ Streaming Video Compression/ Streaming Multimedia-processing		

Services	Standards/Protocols	Implementation Level
Communications Services		
Directory Access E-Mail Messaging Work Flow Management Calendaring Enhanced telephony Shared-screen Teleconferencing Videoconferencing Broadcast		
Document Management Services		
Creating Retrieving Publishing Archiving		
Support Services		
IT Training Help Desk Hardware Installation and Maintenance		
Hardware Services		
Processing Platforms Client Application Data Device Drivers Peripherals Mobile Platforms Storage		

Following the table, a description will be included for each standard, interface, protocol and/or product specification included in the Standards Profile. A suggested format for this description and two examples are given below.

TCP/IP Implementation	TCP/IP and its suite of protocols (IETF STD5,STD7)
Level:	Mandatory adoption
Description:	TCP/IP is a well established, widely adopted industry standard communications protocol. It is the primary means of communications throughout the Internet. TCP/IP provides for a reliable, connection-oriented, end-to-end transport service on top of an unreliable network that can lose, garble, store, and duplicate packets. TCP resembles the OSI Transport Protocol class 4 (TP4), but major differences exist in features, such as handling collisions, addressing format, quality of service, use of user data during set-up of a connection, handling "important data," absence of piggybacking in TP4, kind of message streams, flow control handling, window numbering scheme, and connection release. Associated with TCP is a network layer protocol called Internet Protocol or IP. The IP address structure is inefficiently used at present, which will ultimately result in exhausting Internet addresses. In order to resolve the address limitation problem, IP Version 4 is being revised. The new generation IP (IP Version 6 - also known as IPng) will alleviate the address depletion problems.
Rationale:	Adopting TCP/IP network protocol will simplify communications and data exchange among Internet connected devices and entities. TCP/IP is the only widespread non-proprietary transport protocol standard. TCP/IP supports File Transfer Protocol, Simple Mail Transfer Protocol, and TELNET (remote login). TCP/IP is supported by almost every supplier of communications products.
Implications:	TCP/IP can be used over almost any kind of network to provide quality end-to-end transmission service.

HTML Implementation	Hypertext Markup Language (IETF RFC 1866)
Level:	Mandatory adoption
Description:	The language used to create Web documents and is a subset of Standardized General Markup Language (SGML). Although most browsers display any document written in plain text, there are advantages to writing documents using HTML. When HTML documents are read by applications specifically designed for the Web, they can include formatting, graphics, and links to other documents.

Rationale:	This is the vendor-neutral standard for Web browsers.
Implications:	Cost Effective: Backward compatibility must be considered to ensure cost effectiveness. Allows documents to be easily published and accessed via the Web. Provides the electronic publishing markup for the Web, but does not preserve page fidelity.